IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with <u>underlining</u> and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims 6-9, 11 and 14-19 in accordance with the following:

1-5. (CANCELLED).

6. (CURRENTLY AMENDED)   A terminal device, comprising:

a biometric data storing unit which stores a plurality of kinds of biometric data associated with a person<u>, the plurality of kinds of biometric data including first biometric data used for comparison with biometric data acquired from the person and, second biometric data used for comparison with dictionary data</u>;

a biometric data acquisition unit which acquires one kind of biometric data <u>from said person</u>;

a person authentication unit which authenticates said person based on said acquired one kind of biometric data and <u>the</u> corresponding ~~one~~ <u>first</u> biometric data ~~of~~ <u>among</u> said plurality of kinds of biometric data stored in said biometric data storing unit; and

a biometric data output unit which selects ~~and outputs another~~ <u>the second biometric data having a different</u> kind <u>than said acquired one kind of biometric data,</u> ~~of~~ <u>from the plurality of kinds of</u> biometric data of said person, designated by an authentication device <u>including a dictionary data storing unit storing dictionary data, and outputs the second data</u> from said biometric data storing unit to the authentication device ~~including a dictionary data storing unit storing dictionary data~~, to authenticate said person by matching said ~~another kind of~~ <u>second</u> biometric data with said dictionary data after said person has been authenticated by said person authentication unit.

7. (CURRENTLY AMENDED)   A terminal device as claimed in claim 6, comprising a biometric data processing unit which edits and processes at least partially said <u>second</u> biometric data selected from said biometric data storing unit, wherein said edited and processed <u>second</u> biometric data is output.

8. (CURRENTLY AMENDED)   A terminal device as claimed in claim 6, comprising a biometric data converting unit which converts ~~the~~ a format of said second biometric data selected from said biometric data storing unit, wherein said format-converted second biometric data is output.

9. (CURRENTLY AMENDED)   A terminal device as claimed in claim 6, comprising a corresponding data generating unit which, from said second biometric data selected from said biometric data storing unit, generates corresponding data having a certain bit length and corresponding to said second biometric data, wherein

said generated corresponding second biometric data is output from said biometric data output unit.

10. (ORIGINAL)   A terminal device as claimed in claim 9, comprising a corresponding data parameter generating unit which generates a parameter to be used for generating said corresponding data.

11. (CURRENTLY AMENDED)   A biometric authentication system, comprising:
a terminal device having:
a biometric data storing unit which stores a plurality of kinds of biometric data associated with a person, the plurality of kinds of biometric data including first biometric data used for comparison with biometric data acquired from a person and, second biometric data used for comparison with dictionary data,
a biometric data acquiring unit which acquires one kind of biometric data from said person,
a second person authentication unit which performs person authentication by matching the one kind of biometric data acquired by the biometric data acquiring unit with ~~a~~ the corresponding ~~one of~~ first biometric data among the plurality of kinds of biometric data stored in the biometric data storing unit, and
a biometric data transmitting unit which outputs the second biometric data having a ~~at least another~~ different kind ~~of biometric data when~~ than said acquired one kind of biometric data, from the plurality of biometric data of said person stored in the storing unit, after said person has been authenticated by the second person authentication unit; and
an authentication device having:

3

a dictionary data storing unit which stores biometric data as dictionary data to be used for authentication~; and

a first person authentication unit which performs first person-authentication based on comparing said at least one another kind of second biometric data transmitted from said biometric data transmitting unit, and said dictionary data stored in said dictionary data storing unit.

12-13. (CANCELLED).

14. (CURRENTLY AMENDED)   A biometric authentication system as claimed in claim 11, wherein:

said first authentication device comprises a corresponding data generating unit which, based on said second biometric data transmitted from said biometric data transmitting unit, generates corresponding data having a certain bit length and corresponding to said second biometric data, and

specific dictionary data stored in said dictionary data storing unit is located by using said generated corresponding data, and said first person authentication unit performs said first person authentication based on said specific dictionary data and said transmitted second biometric data.

15. (CURRENTLY AMENDED)   A biometric authentication system as claimed in claim 14, wherein when said first person authentication based on said specific dictionary data cannot be performed,~ said~ first authentication device performs said first person authentication based on all of said dictionary data stored in said dictionary data storing unit and said transmitted second biometric data.

16. (CURRENTLY AMENDED)   A biometric authentication system as claimed in claim 11, wherein:

said terminal device includes a first~ biometric data processing unit, which edits and processes at least partially said~ second biometric data selected from said biometric data storing unit, and a first processing data storing unit, which stores data that said first ~biometric data processing unit uses to edit and process said second biometric data,

said authentication device includes a second biometric data processing unit, which edits and processes said dictionary data at least partially, and a second processing data storing unit,

4

which stores data that said second biometric data processing unit uses to edit and process said dictionary data, and

said first person authentication unit performs said first person authentication based on said edited and processed second biometric data and said edited and processed dictionary data.

17. (CURRENTLY AMENDED)   A biometric authentication system as claimed in claim 11, wherein:

said authentication device comprises a conversion data storing unit, which stores~conversion data concerning said second biometric data used in said first person authentication unit,

said terminal device comprises a biometric data converting unit which converts-the a format of said second biometric data stored in said biometric data storing unit, and

said biometric data converting unit converts the format of said second biometric data by using said format data transmitted from said conversion data storing unit, and said format-converted second biometric data is transmitted to said authentication device.

18. (CURRENTLY AMENDED)   A biometric authentication system as claimed in claim 11, wherein said terminal device further comprises:

a first corresponding data generating unit which generates first corresponding data having a certain bit length and corresponding to specific the second biometric data selected from along-said plurality of biometric data stored in said biometric data storing unit, and a corresponding data transmitting unit which transmits out said generated first corresponding data; and

said authentication device further comprises a second corresponding data generating unit which generates second corresponding data having a certain bit length and corresponding to said dictionary data, wherein

said first person authentication unit performs first person authentication based on said transmitted first corresponding data and said second corresponding data.

19. (CURRENTLY AMENDED)   A biometric authentication system as claimed in claim 18, wherein:

said terminal device includes a biometric data acquisition unit which acquires biometric data and a second person authentication unit which performs second person authentication, and

said second person authentication is performed using said acquired biometric data and

said biometric data stored in said biometric data storing unit and, when the identity of said person has been authenticated, said first corresponding data to be used in said first person authentication unit is transmitted to said authentication device.

20. (PREVIOUSLY PRESENTED)   A biometric authentication system as claimed in claim 19, wherein:

said terminal device includes a first corresponding data parameter generating unit which generates a corresponding data parameter to be used for generating said corresponding data, and

said generated corresponding data parameter is not only used in said first corresponding data generating unit, but also transmitted to said authentication device and used in said second corresponding data generating unit.

21. (PREVIOUSLY PRESENTED)   A biometric authentication system as claimed in claim 19, wherein:

said authentication device includes a second corresponding data parameter generating unit which generates a corresponding data parameter to be used for generating said corresponding data, and

said generated corresponding data parameter is not only used in said second corresponding data generating unit, but also transmitted to said terminal device and used in said first corresponding data generating unit.

22. (ORIGINAL)   A biometric system as claimed in claim 18, wherein said authentication device encrypts data that said person has by using said corresponding data used for authentication of said person as an encryption key.

23-26. (CANCELLED).

27. (PREVIOUSLY PRESENTED)   A biometric data acquisition system, comprising:
      a terminal device having a biometric data storing unit for storing a plurality of kinds of biometric data associated with a person;
      an authentication device which performs person authentication based on said biometric data transmitted, from said terminal device; and
      a biometric data acquisition device having

a biometric data acquiring unit for acquiring said biometric data,

an encryption unit which encrypts said biometric data by using an encryption key and

a decryption key storing unit which stores a decryption key, and wherein

said biometric data associated with said person, acquired by said biometric data acquiring unit, is encrypted by said encryption unit and transferred to said terminal device for storage in said biometric data storing unit,

when said encrypted biometric data stored in said terminal is transmitted to said authentication device, said authentication device decrypts said encrypted biometric data by using said decryption key stored in said decryption key storing unit of said biometric data acquisition device, and

when said decryption key is used by said authentication device, said biometric data acquisition device charges a fee to said authentication device for said use.

28. (PREVIOUSLY PRESENTED) A biometric data acquisition system, comprising:

a terminal device having a biometric data storing unit for storing a plurality of kinds of biometric data associated with a person;

an authentication device which performs person authentication based on said biometric data transmitted, from said terminal device; and

a biometric data acquisition device having a biometric data acquiring unit for acquiring said biometric data, an encryption unit which encrypts said biometric data by using an encryption key and a decryption key storing unit which stores a decryption key, and wherein

said biometric data associated with said person, acquired by said biometric data acquiring unit, is encrypted by said encryption unit and transferred to said terminal device for storage in said biometric data storing unit,

when said encrypted biometric data stored in said terminal is transmitted to said authentication device, said authentication device decrypts said encrypted biometric data by using said decryption key stored in said decryption key storing unit of said biometric data acquisition device, and

said biometric data acquisition device charges a fee to said authentication device according to the number of times that said biometric data stored into said terminal device by said biometric data acquisition device is used by said authentication device.